Reference Incident Classification Taxonomy Task Force Update

Rossella Mattioli and Yonas Leguesse, ENISA

Talking about taxonomies

- ENISA Report: Detect, SHARE, Protect - Solutions for Improving Threat Data Exchange among CSIRTs (Nov 2013)
  https://www.enisa.europa.eu/publications/detect-share-protect-solutions-for-improving-threat-data-exchange-among-certs

- ENISA Report: Information sharing and common taxonomies between CSIRTs and Law Enforcement (Dec 2015)
  https://www.enisa.europa.eu/publications/information-sharing-and-common-taxonomies-between-csirts-and-law-enforcement/

- ENISA Report: A good practice guide of using taxonomies in incident prevention and detection (Dec 2016)
  https://www.enisa.europa.eu/publications/using-taxonomies-in-incident-prevention-detection/

- Taxonomy: Common Taxonomy CSIRT-LEA Cooperation
  https://www.europol.europa.eu/publications-documents/common-taxonomy-for-law-enforcement-and-csirts

- Taxonomy: eCSIRT.net (adapted) Taxonomy
  https://www.trusted-introducer.org/Incident-Classification-Taxonomy.pdf

Reference Incident Classification Taxonomy

https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy

Problems…just to name a few

- There are many terms
- There are many taxonomies
- There are different versions of the same taxonomy
- Different references to the same taxonomy often point to different taxonomy versions!

Why ?

- Taxonomy for CSIRT technical incidents
- To ensure that CSIRTs are speaking the same language.
- To facilitate sharing across CSIRTs.
- To facilitate the harmonization of statistics between the CSIRT community.
- To facilitate translation between different taxonomies, without disruption or need for major overhaul.
- Could be useful mapping within the context of NIS directive.
- Get ready for automated info exchange

Reference Taxonomy Task Force

- Develop Reference Incident Classification Taxonomy for CSIRTs in Europe
- Define and develop an Update and Versioning Mechanism
- Host reference document
- Organise regular physical meetings with the stakeholders

Reference Taxonomy Task Force Current Members

ALEF-CSIRT

BSI/CERT-Bund

CaixaBank

CCN-CERT

CERT.AT

CERT.be

CERT.LV/TF-CSIRT

CERT-Bund

CERT-SE

CESNET

CIRCL.lu

DFN-CERT

EATM-CERT

EC3

EGI-CSIRT

ENISA

Eurocontrol

Gemalto

GOVCERT.LU

IRIS-CERT

KBC Group CERT

Open Systems

S-CURE

SI-CERT

Siemens

SWITCH CERT

Tallinn University

Telia CERT

UK MOD / University of Warwick

Timeline

https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy

eCSIRT.net mkVI (starting point)

- First version 2003
- Good starting point
- Main categories are still current, practical and universal
- Could be easily used to map other existing taxonomies

REFERENCE TAXONOMY (ECSIRT.NET)[10]
Abusive Content
Malicious Code
Information Gathering
Intrusion Attempts
Intrusion
Availability
Information Content Security
Fraud
Vulnerable
Other
Test

https://www.trusted-introducer.org/Incident-Classification-Taxonomy.pdf

Common Taxonomy CSIRT-LEA

COMMON TAXONOMY FOR LE AND CSIRTS
Abusive Content
Malware
Information Gathering
Intrusion Attempts
Intrusion
Availability
Information Security
Fraud
Other

- Adaptation of the CERT.PT taxonomy, which is itself an adaptation of the eCSIRT.net mkVI taxonomy.
- Used in the context of law enforcement
- It has been extended to also include a mapping of the incident classifications with a legal framework.
- Resulted from CSIRT LEA annual workshop and it is constantly updated and reviewed by the taxonomy governance group TGG
- Members of the TGG are part of the reference taxonomy task force to ensure sync & synergies

https://www.europol.europa.eu/sites/default/files/documents/common_taxonomy_for_the_national_network_of_csirts.pdf

eCSIRT mapped to Common CSIRT LEA

REFERENCE TAXONOMY (ECSIRT.NET)[10]	COMMON TAXONOMY FOR LE AND CSIRTS	NOTE
Abusive Content	Abusive Content	
Malicious Code	Malware	
Information Gathering	Information Gathering	
Intrusion Attempts	Intrusion Attempts	
Intrusion	Intrusion	
Availability	Availability	
Information Content Security	Information Security	
Fraud	Fraud	
Vulnerable		Not relevant to LEA
Other	Other	
Test		Not relevant to LEA

Table 2: Reference taxonomy vs Common Taxonomy for LE and CSIRTs

LEGEND	
	The same
	Not mentioned in the other taxonomy
	Not present

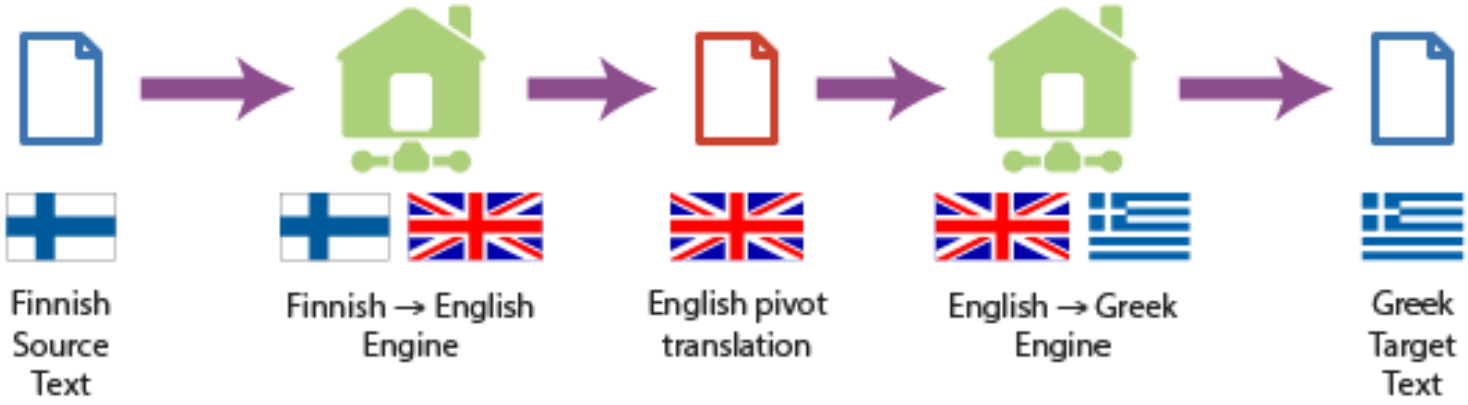
eCSIRT mapped to CIRCL

CIRCL TAXONOMY	REFERENCE TAXONOMY
Spam	Abusive Content
malware	Malicious Code
Scan	Information Gathering
	Intrusion Attempts
system-compromise	Intrusions
XSS	
sql-injection	
denial-of-service	Availability
information-leak	Information Content Security
copyright-issue	Fraud
phishing,	
Scam	
vulnerability	Vulnerable
Fastflux	Other
	Test

Table 5: CIRCL taxonomy vs Reference Taxonomy

LEGEND	
	The same
	Similar but with some differences
	The same but in a different category
	Not mentioned in the other taxonomy

Pivot Translation



Reference taxonomy as a pivot language to map existing taxonomies and facilitate info exchange.

Pivot Mapping

Next steps

Decide on two elemental points

- Confirm eCSIRT.net as starting point
- Decide on the granularity of the sub levels

Review and consolidate Incident Classifications and definitions in the reference taxonomy

Define update workflow and versioning mechanism

Decide about the hosting of the reference taxonomy

Propose way forward, e.g.: to meet periodically

Thank you

https://www.enisa.europa.eu/csirts-in-europe
https://www.enisa.europa.eu/csirts-map
https://www.enisa.europa.eu/csirt-community
https://www.enisa.europa.eu/csirt-services

CSIRT-Relations@enisa.europa.eu